(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 823 803 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
11.02.1998 Patentblatt 1998/07

(51) Int. Cl.[6]: **H04L 12/28**, H04L 12/22, H04L 29/06

(21) Anmeldenummer: **96112872.5**

(22) Anmeldetag: **09.08.1996**

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV SI

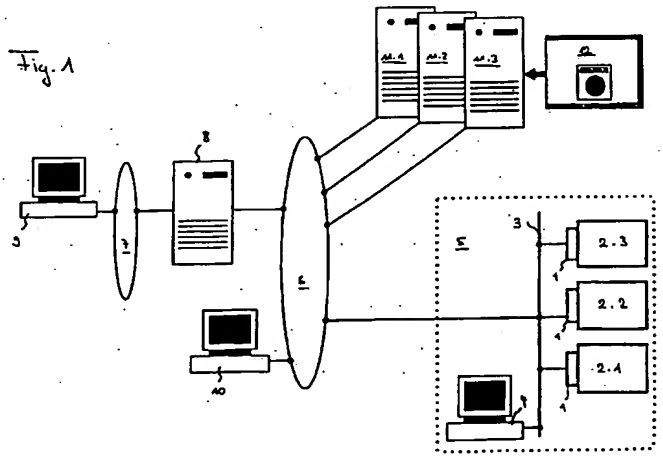
(71) Anmelder:
Landis & Gyr Technology Innovation AG
6301 Zug (CH)

(72) Erfinder:
- **Copley, Jonathan Miles**
  6330 Cham (CH)
- **Skipper, Philip Robert**
  6318 Walchwil (CH)

(54) Einrichtung zum Zugriff auf ein an ein lokales Netzwerk angeschlossenes Gerät über ein öffentliches Netzwerk

(57) Eine Einrichtung zum Zugriff auf ein an ein lokales Netzwerk (5) angeschlossenes Gerät (2.1; 2.2; 2.3) über ein an einem öffentliches Netzwerk (6) angeschlossene Station (10; 9; 4) weist eine Schnittstelleneinrichtung (1) auf, über die das Gerät (2.1; 2.2; 2.3) für einen Datenaustausch zugreifbar ist, wobei die Schnittstelleneinrichtung (1) Mittel zur Interpretierung und zur Ausführung eines Befehles aufweist, der über die am öffentlichen Netzwerk angeschlossene Station (10; 9; 4) auslösbar ist und durch den die Funktionalität des Gerätes (2.1; 2.2; 2.3) steuerbar oder programmierbar ist oder durch den Daten des Gerätes (2.1; 2.2; 2.3) abfragbar sind. Die Schnittstelleneinrichtung (1) umfasst zudem Mittel zur Prüfung der Authentizität des Befehles. Die Einrichtung erlaubt die sichere Fernprogrammierung insbesondere auch von Geräten bzw. Teilen einer Anlage über ein öffentliches Netzwerk (6), wobei beispielhaft Heizungs-, Lüftungs- und Klimaanlagen, Zutritts- und Feuerüberwachungssysteme oder allgemein Gebäudeautomatisationsanlagen - die auch als Gebäudeleitsysteme bezeichnet werden - genannt seien.

Fig. 1



EP 0 823 803 A1

Beschreibung

Die Erfindung bezieht sich auf eine Einrichtung gemäss dem Oberbegriff des Anspruchs 1.

Solche Einrichtungen eignen sich beispielsweise zur Fernprogrammierung von Geräten zur Steuerung oder Regelung von Klimagrössen eines Raumes über ein öffentliches Datennetzwerk oder allgemein zum Datenaustausch zwischen einer an einem öffentlichen Datennetzwerk angeschlossenen Station und einem über das öffentliche Datennetzwerk zugreifbaren Gerät.

Es ist eine Einrichtung dieser Art bekannt (WO 9605681 A1), bei der eine an einem lokalen Datennetz angeschlossene Datenbasis über einen Server von einer an einem öffentlichen Datennetz angeschlossenen Station aus über das öffentliche Datennetz zugreifbar ist.

Es sind auch Einrichtungen und Verfahren bekannt (EP 686 905 A1 oder EP 693 836 A1), durch welche die Authentizität eines Datentransfers in einem öffentlichen Datennetz sichergestellt werden können.

Der Erfindung liegt die Aufgabe zugrunde, eine Einrichtung zu schaffen, mit der die Funktionalität eines Gerätes von einer Station aus über ein öffentliches Netzwerk - beispielsweise über das Internet - mit der erforderlichen Sicherheit programmierbar ist und mit der Daten des Gerätes über das öffentliche Netzwerk sicher übertragbar und auf der Station darstellbar sind.

Die genannte Aufgabe wird erfindungsgemäss durch die Merkmale des Anspruchs 1 gelöst. Vorteilhafte Ausgestaltungen ergeben sich aus den abhängigen Ansprüchen.

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand der Zeichnung näher erläutert.

Es zeigen:

Fig. 1 eine Einrichtung mit Geräten, deren Funktionalität von verschiedenen Stationen aus über ein öffentliches Netz steuerbar ist,

Fig. 2 eine Schnittstelleneinrichtung für ein steuerbares Gerät,

Fig. 3 eine Einheit der Schnittstelleneinrichtung,

Fig. 4 ein Datenflussdiagramm zur Einrichtung,

Fig. 5 der Datenfluss einer ersten Variante der Einrichtung,

Fig. 6 der Datenfluss einer zweiten Variante der Einrichtung,

Fig. 7 der Datenfluss einer dritten Variante der Einrichtung und

Fig. 8 eine Variante der Schnittstelleneinrichtung.

In der Fig. 1 bedeutet 1 eine Schnittstelleneinrichtung für ein Gerät 2, welches typischerweise eine Einrichtung 2.1 zur Steuerung oder Regelung einer Klimagrösse eines Raumes oder eines Gebäudes oder dann ein Videorecorder 2.2 oder eine Waschmaschine 2.3 ist.

In einem vorteilhaften Aufbau der Einrichtung ist das Gerät 2 bzw. 2.1, 2.2 oder 2.3 durch die Schnittstelleneinrichtung 1 an einem Kommunikationsmedium 3 angeschlossen, das vorteilhafterweise auch mit einem Terminal 4 verbunden ist. Das Kommunikationsmedium 3, das Terminal 4 und die Ausführungen 2.1, 2.2 und 2.3 des Gerätes 2 bilden ein lokales Datenkommunikationsnetzwerk 5. Das Kommunikationsmedium 3 des lokalen Datenkommunikationsnetzwerkes 5 ist typischerweise ein Hausbus. Im allgemeinen ist das Kommunikationsmedium 3 eine Drahtverbindung oder eine drahtlose Verbindung.

Das Terminal 4 ist vorzugsweise ein Personalcomputer.

Das lokale Datenkommunikationsnetzwerk 5 ist mit einem öffentlichen Datenkommunikationsnetz 6 verbunden. Typischerweise ist mindestens ein weiteres lokales Datenkommunikationsnetz 7 über einen Kommunikationscomputer 8 mit dem öffentlichen Datenkommunikationsnetz 6 verbunden, wobei am Datenkommunikationsnetz 7 wenigstens ein weiteres Terminal 9 angeschlossen ist.

Die Schnittstelleneinrichtung 1 ist mit Vorteil so ausgestaltet, dass das Gerät 2 bzw. 2.1, 2.2 oder 2.3 sowohl vom Terminal 4 des lokalen Datenkommunikationsnetzwerkes 5 als auch vom Terminal 9 des weiteren lokalen Datenkommunikationsnetzes 8 oder von einer beliebigen am öffentlichen Datenkommunikationsnetzwerk 6 angeschlossenen Station 10 aus für einen sicheren Datenaustausch zugreifbar ist.

Mit Vorteil ist über das öffentliche Datenkommunikationsnetzwerk 6 mindestens eine weitere Computereinheit 11.1, 11.2 oder 11.3 erreichbar, auf der eine dem Gerät 2, 2.1, 2.2 oder 2.3 zugeordnete Datenbasis 12 abgespeichert ist, wobei Daten der Datenbasis 12 mindestens auszugsweise in einem Ausgabefenster bzw. Window auf dem Terminal 4 oder 9 und auch auf der Station 10 darstellbar sind.

Die Schnittstelleneinrichtung 1 weist ein Sicherheitsmodul 20 (Fig. 2) auf, welches vorteilhafterweise mit einem ersten Kommunikationsmodul 21 und einem zweiten Kommunikationsmodul 22 verbunden ist, wobei das erste Kommunikationsmodul 21 mindestens ein Teil der Schnittstelle zwischen dem Sicherheitsmodul 20 und dem Kommunikationsmedium 3 und das zweite Kommunikationsmodul 22 mindestens ein Teil der Schnittstelle zwischen dem Sicherheitsmodul 20 und dem Gerät 2 bzw. 2.1, 2.2 oder 2.3 ist.

Sofern das Kommunikationsmedium 3 ein elektrischer Leiter ist, weist die Schnittstelleneinrichtung 1 zudem ein entsprechendes Steckerelement 23 zum Anschliessen der Schnittstelleneinrichtung 1 an das

Kommunikationsmedium 3 (Fig. 1) auf. Die Schnittstelleneinrichtung 1 ist typischerweise über ein weiteres Steckerelement 24 mit dem Gerät 2 bzw. 2.1, 2.2 oder 2.3 verbindbar. Bei Bedarf ist die Schnittstelleneinrichtung 1 jedoch nicht galvanisch über das weitere Steckerelement 24, sondern auf eine andere Art, beispielsweise über einen modulierbaren Lichtstrahl mit dem Gerät 2 bzw. 2.1, 2.2 oder 2.3 koppelbar.

Die Art der Kommunikationsmodule 21 und 22 ist selbstverständlich auf die eingesetzten Übertragungsprotokolle und die verwendeten Übertragungsmittel abgestimmt. Das erste Kommunikationsmodul 21 ist beispielsweise ein elektronischer Baustein zur Durchführung des Protokolls TCP/IP (Transmission Control Protocol/Internet Protocol) während das zweite Kommunikationsmodul 22 beispielsweise ein elektronischer Baustein zur Durchführung des Übertragungsprotokolls des sogenannten PROFIBUS (Process Field Bus; DIN 19 245) ist.

Mit Vorteil umfasst das Sicherheitsmodul 20 erste Mittel 31 (Fig. 3) zur Bedienung des ersten Kommunikationsmoduls 21 (Fig. 2), zweite Mittel 32 (Fig. 3) zur Bedienung des zweiten Kommunikationsmoduls 22 (Fig. 2), dritte Mittel 33 (Fig.3) zur Decodierung einer Netzwerkadresse, vierte Mittel 34 zur Verschlüsselung und Entschlüsselung von Daten und fünfte Mittel 35 zur Interpretierung und Ausführung von Befehlen, welche an das mit der Schnittstelleneinrichtung 1 verbundene Gerät 2 bzw. 2.1, 2.2 oder 2.3 gerichtet sind.

In Fig. 4, Fig. 5, Fig. 6 und Fig. 7 sind die wesentlichen Datenflüsse zwischen der Station 10, der Schnittstelleneinrichtung 1 und dem Gerät 2 dargestellt, wobei in Fig. 5 bis Fig. 7 auch die auf der Computereinheit 11.1 oder 11.2 oder 11.3 (Fig. 1) verwirklichte Datenbasis 12 einbezogen ist.

In der für Fig. 4 bis Fig. 7 gewählten, aus der Literatur bekannten Darstellungsart für Datenflussdiagramme (dazu beispielsweise D. J. Hatley, I. A. Pirbhai: Strategies for Real-Time System Specification, Dorset House, NY 1988) bedeutet ein Kreis eine Aktivität, ein Viereck allgemein ein System und ein Pfeil einen Kanal zur Übertragung von Daten und/oder Ereignissen, wobei eine Pfeilspitze in die wesentliche Datenflussrichtung zeigt. Ein Datenspeicher, der allgemein mehreren Aktivitäten zur Verfügung steht, ist durch zwei gleich lange, parallele Linien dargestellt. Mit dem Begriff Datenspeicher wird hier eine Einrichtung zur Speicherung von Daten bezeichnet, welche auch Mittel zur Verhinderung von Konflikten bei zeitlich parallelem Zugriff mehrerer Aktivitäten auf die Daten aufweist. Im weiteren ist beispielsweise eine Anordnung aus zwei durch einen Kanal verbundenen Aktivitäten mit einer einzigen Aktivität, welche alle Aufgaben der besagten beiden Aktivitäten erfüllt, äquivalent. Eine Aktivität ist allgemein in mehrere über Kanäle und/oder Datenspeicher verbundene Aktivitäten zerlegbar. Weitere in der Literatur der Datenflussdiagramme benutzte Bezeichnungen sind "Terminator" für das angrenzende System, "Process" oder "Task" für die Aktivität, "Data Flow" oder "Channel" für den Kanal und "Pool" oder "Data Pool" für den Datenspeicher.

Eine Aktivität kann als elektronische Schaltung oder auch softwaremässig als Prozess, Programmstück oder Routine verwirklicht werden, wobei die Aktivität bei einer softwaremässigen Ausführung auch die Zielhardware umfasst.

Die Station 10 weist eine erste Aktivität 40 sowie mit Vorteil einen über einen Kanal 41 mit der ersten Aktivität 40 verbundenen ersten Datenspeicher 42 zur Speicherung von Information für kryptographische Methoden auf.

Ein durch einen Bediener der Station 10 eingegebener Befehl B für das Gerät 2, wird von der ersten Aktivität 40 mit bekannten kryptographische Methoden verschlüsselt über einen Kanal 43 an eine zweite, in der Schnittstelleneinrichtung 1 verwirklichte Aktivität 44 übermittelt, wobei der Kanal 43 über das öffentliche Datenkommunikationsnetz 6 (Fig. 1) aufgebaut wird. Der an die zweite Aktivität 44 übermittelte Befehl B wird interpretiert und ausgeführt, indem die zweite Aktivität 44 ein gewisses auf Eigenschaften des Gerätes 2 abgestimmtes Datentelegramm T aufbereitet und über einen Kanal 45 an das Gerät 2 übermittelt. Bei Bedarf wird eine Antwort des Gerätes 2 auf das Datentelegramm T über den Kanal 45 an die Schnittstelleneinrichtung 1 und von da über den Kanal 43 an die Station 10 übermittelt.

Zum Schutz gegen allfälligen Missbrauch werden die zwischen der Station 2 und der Schnittstelleneinrichtung 1 ausgetauschten Daten im öffentlichen Datenkommunikationsnetzwerk 6 mit Vorteil derart verschlüsselt übertragen, dass auch die Authentizität der Daten gesichert ist. Durch die Funktionalität des Sicherheitsmodules 20, welche insbesondere mit den ersten Mitteln 31 (Fig. 3) und den zweiten Mitteln 32 die Codierung/Decodierung von Protokollen und mit den Mitteln 34 kryptographische Verfahren zur Übertragung von Daten über das öffentliche Datenkommunikationsnetzwerk 6 umfasst ist ein hoher Sicherheitsstandard für die Fernbedienung erreichbar.

Für eine bedienerfreundliche Benutzerführung auf der Station 10 ist die über das öffentliche Datenkommunikationsnetzwerk 6 (Fig. 1) verfügbare Datenbasis 12 einsetzbar.

In der Datenbasis 12 sind wesentliche Daten zur Bedienung, Programmierung und Steuerung des Gerätes 2 bzw. 2.1 bzw. 2.2 bzw. 2.3 abgespeichert. Die Datenbasis wird beispielsweise durch den Hersteller des Gerätes 2 bzw. 2.1 bzw. 2.2 bzw. 2.3 im öffentlichen Datenkommunikationsnetzwerk 6 eingerichtet und Benutzern des Gerätes 2 bzw. 2.1 bzw. 2.2 bzw. 2.3 die Fernbedienung zur Verfügung gestellt.

In einer vorteilhaften Ausgestaltung der Datenbasis 12 sind die zur Bedienung, Programmierung und Steuerung des Gerätes 2 bzw. 2.1 bzw. 2.2 bzw. 2.3 notwendigen Daten von der Station 10 aus in übersichtlicher

Form einsichtbar und bei Bedarf durch den Benutzer der Station 10 veränderbar. Falls das öffentliche Datenkommunikationsnetzwerk 6 das Internet ist, ist mindestens ein Teil der Datenbasis mit Vorteil als sogenannte Web-Site verfügbar.

In einer ersten Variante (Fig. 5) der Einrichtung wird von der ersten Aktivität 40 aus ein Kanal 46 über das öffentliche Datenkommunikationsnetzwerk 6 zur Datenbasis 12 aufgebaut. Durch die über den Kanal 46 verfügbare Datenbasis 12 wird eine bedienungsgerechte Benutzerführung auf der Station 10 ermöglicht. Die zwischen der Station 10 und dem Gerät 2 aufbaubaren Kanäle 43 und 45 sind bidirektional, so dass auch aktuelle Gerätedaten auf der Station 10 abbildbar sind.

In einer zweiten Variante (Fig. 6) der Einrichtung wird von der ersten Aktivität 40 aus ein Kanal 47 über das öffentliche Datenkommunikationsnetzwerk 6 zur Datenbasis 12 aufgebaut. Ein von der Station 10 an die Datenbasis 12 übertragener Befehl zur Bedienung, Programmierung oder Steuerung des Gerätes 2 bzw. 2.1 bzw. 2.2 bzw. 2.3 wird durch eine der Datenbasis 12 zugeordnete Aktivität 48 aufbereitet und über einen weiteren Kanal 49 an die Schnittstelleneinrichtung 1 und von da an das Gerät 2 übertragen, wobei die Kanäle 47, 49 und 45 bidirektional sind, so dass auch aktuelle Gerätedaten auf der Station 10 abbildbar sind.

In einer dritten Variante (Fig. 7) der Einrichtung wird eine bedienungsgerechte Benutzerführung auf der Station 10 dadurch ermöglicht, dass die in der Schnittstelleneinrichtung 1 verwirklichte zweite Aktivität 44 einen Kanal 50 zur Datenbasis 12 aufbaut.

Statt der in Fig. 5, Fig. 6 und Fig. 7 dargestellten Station 10 sind zur Bedienung, Programmierung und Steuerung des Gerätes 2 bzw. 2.1 bzw. 2.2 bzw. 2.3 selbstverständlich auch das Terminal 4 (Fig. 1) und das weitere Terminal 9 einsetzbar.

Die Schnittstelleneinrichtung 1 mit dem Sicherheitsmodul 20 ermöglicht eine sichere, kostengünstige und benutzerfreundliche Fernbedienung, Fernprogrammierung und Fernsteuerung des Gerätes 2 bzw. 2.1 bzw. 2.2 bzw. 2.3 über das öffentliche Datenkommunikationsnetzwerk 6. Im Sicherheitsmodul 20 ist als hochintegrierter Baustein herstellbar. Das Sicherheitsmodul 20 ist vollständig als sogenannter Hardware-Chip verwirklichbar, wodurch die erreichbare Sicherheit wesentlich erhöht werden kann.

In der Fig. 8 ist mit 60 eine Ausführungsvariante der Schnittstelleneinrichtung 1 (Fig. 1) bezeichnet. Die Ausführungsvariante 6 weist grundsätzlich die in der Fig. 3 dargestellte Funktionalität auf, ist jedoch derart aufgebaut, dass sie funktional zwischen das öffentliche Datenkommunikationsnetzwerk 6 und das lokale Datenkommunikationsnetzwerk 5 einfügbar ist. Die Ausführungsvariante 60 der Schnittstelleneinheit ist insbesondere dann vorteilhaft, wenn die zu bedienenden Geräte 2 bzw. 2.1, 2.2 und 2.3 des lokalen Datenkommunikationsnetzwerkes 5 gleichartige Bedienkonzepte aufweisen.

Die vorgeschlagene Einrichtung mit der Schnittstelleneinrichtung 1 bzw. 60 zum Zugriff auf das Gerät 2 erlaubt die sichere Fernprogrammierung insbesondere auch von Geräten bzw. Teilen einer Anlage, wobei beispielhaft Heizungs-, Lüftungs- und Klimaanlagen, Zutritts- und Feuerüberwachungssysteme oder allgemein Gebäudeautomatisationsanlagen - die auch als Gebäudeleitsysteme bezeichnet werden - genannt seien.

Patentansprüche

1. Einrichtung zum Zugriff auf ein an ein lokales Netzwerk (5) angeschlossenes Gerät (2.1; 2.2; 2.3) über ein an einem öffentliches Netzwerk (6) angeschlossene Station (10; 9; 4), wobei das lokale Netzwerk (5) mit dem öffentlichen Netzwerk (6) verbunden ist, **gekennzeichnet durch**

   eine Schnittstelleneinrichtung (1; 60), über die das Gerät (2.1; 2.2; 2.3) für einen Datenaustausch zugreifbar ist, wobei die Schnittstelleneinrichtung (1; 60) Mittel (35) zur Interpretierung und zur Ausführung eines Befehles aufweist, der über die am öffentlichen Netzwerk angeschlossene Station (10; 9; 4) auslösbar ist und durch den die Funktionalität des Gerätes (2.1; 2.2; 2.3) steuerbar oder programmierbar ist oder durch den Daten des Gerätes (2.1; 2.2; 2.3) abfragbar sind und wobei die Schnittstelleneinrichtung (1; 60) zudem Mittel (34) zur Prüfung der Authentizität des Befehles aufweist.

2. Einrichtung nach Anspruch 1, **dadurch gekennzeichnet,**

   dass die Schnittstelleneinrichtung (1; 60) und die Station (10; 9; 4) Mittel (40, 42; 34) zur Verschlüsselung und Entschlüsselung von Daten aufweisen, so dass ein zwischen der Station (10; 9; 4) und der Schnittstelleneinrichtung (1) über das öffentliche Netzwerk (6) übertragener Datenstrom verschlüsselbar ist.

3. Einrichtung nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,**

   dass eine über das öffentliche Netzwerk (6) zugreifbare Datenbasis (12) verfügbar ist, welche Daten zur Führung eines Bedieners der Station (10; 9; 4) aufweist.

4. Einrichtung nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,**

   dass ein von der Schnittstelleneinrichtung (1; 60) interpretierbare Befehlssatz in einer über

das öffentliche Netzwerk (6) zugreifbaren Datenbasis (12) verfügbar ist.

5. Einrichtung nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,**

dass die Schnittstelleneinrichtung (1; 60) Mittel (21, 31) zur Codierung/Decodierung eines Protokolls zur Übertragung von Daten über das öffentliche Netzwerk (6) aufweist.

6. Einrichtung nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,**

dass die Schnittstelleneinrichtung (1; 60) Mittel (22, 32) zur Kommunikation mit dem Gerät (2.1; 2.2; 2.3) aufweist.

7. Einrichtung nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,**

dass das Gerät (2.1) eine Einrichtung zur Steuerung oder Regelung von Klimagrössen eines Raumes ist.

8. Einrichtung nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,**

dass die Schnittstelleneinrichtung (1) zwischen das Kommunikationsmedium (3) und das Gerät (2.1; 2.2; 2.3) geschaltet ist.

9. Einrichtung nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet,**

dass die Schnittstelleneinrichtung (60) zwischen das lokale Kommunikationsnetzwerk (5) und das öffentliche Datenkommunikationsnetz (6) geschaltet ist.

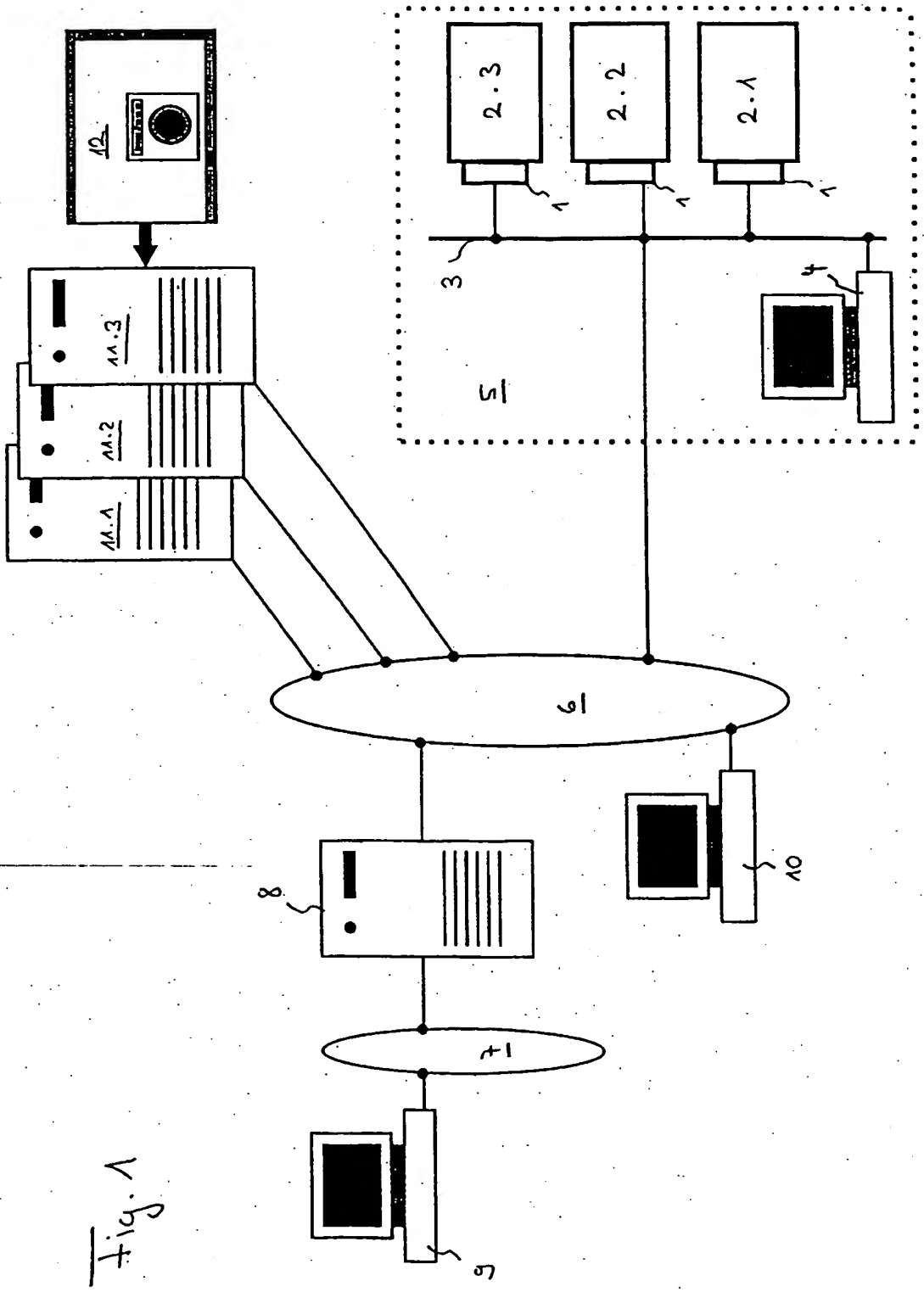
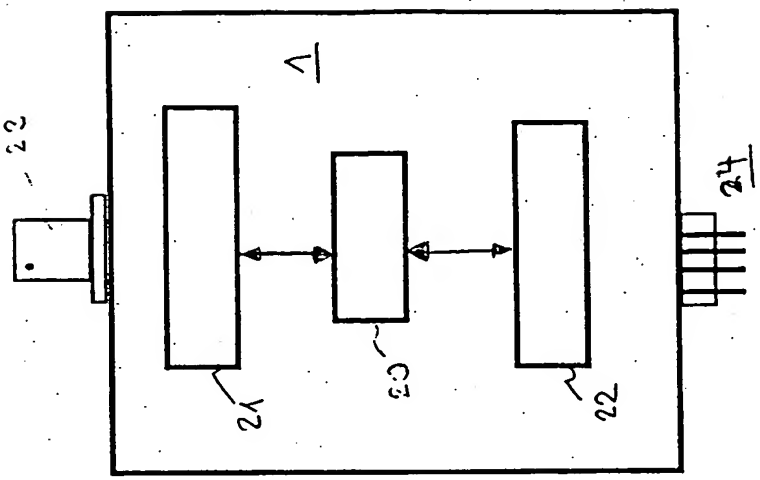


Fig. 1

Fig. 2



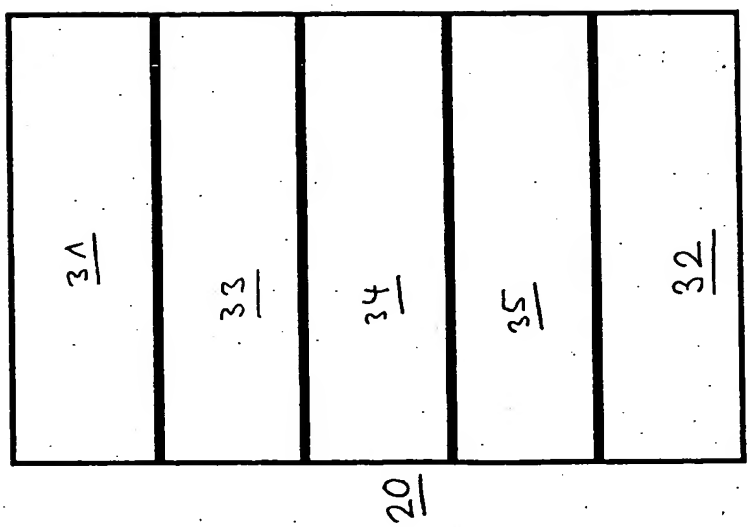


Fig. 3

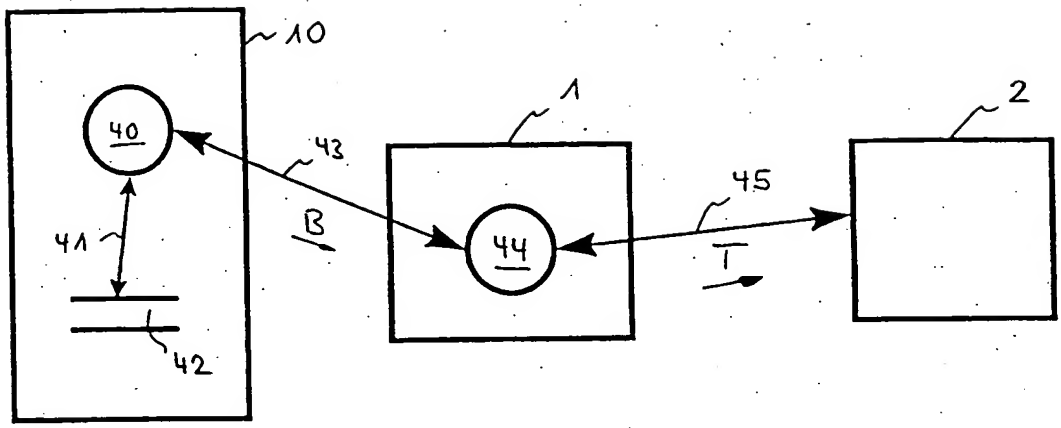


Fig. 4

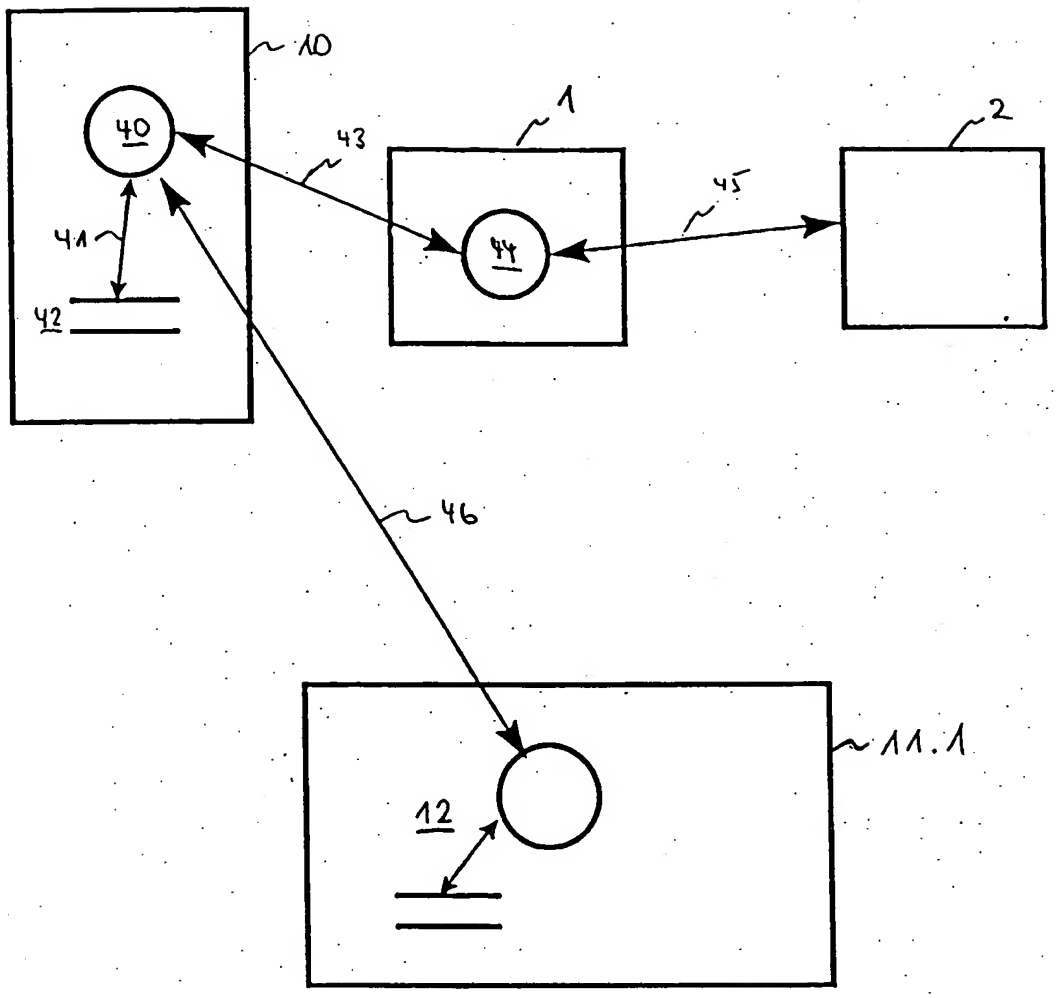


Fig. 5

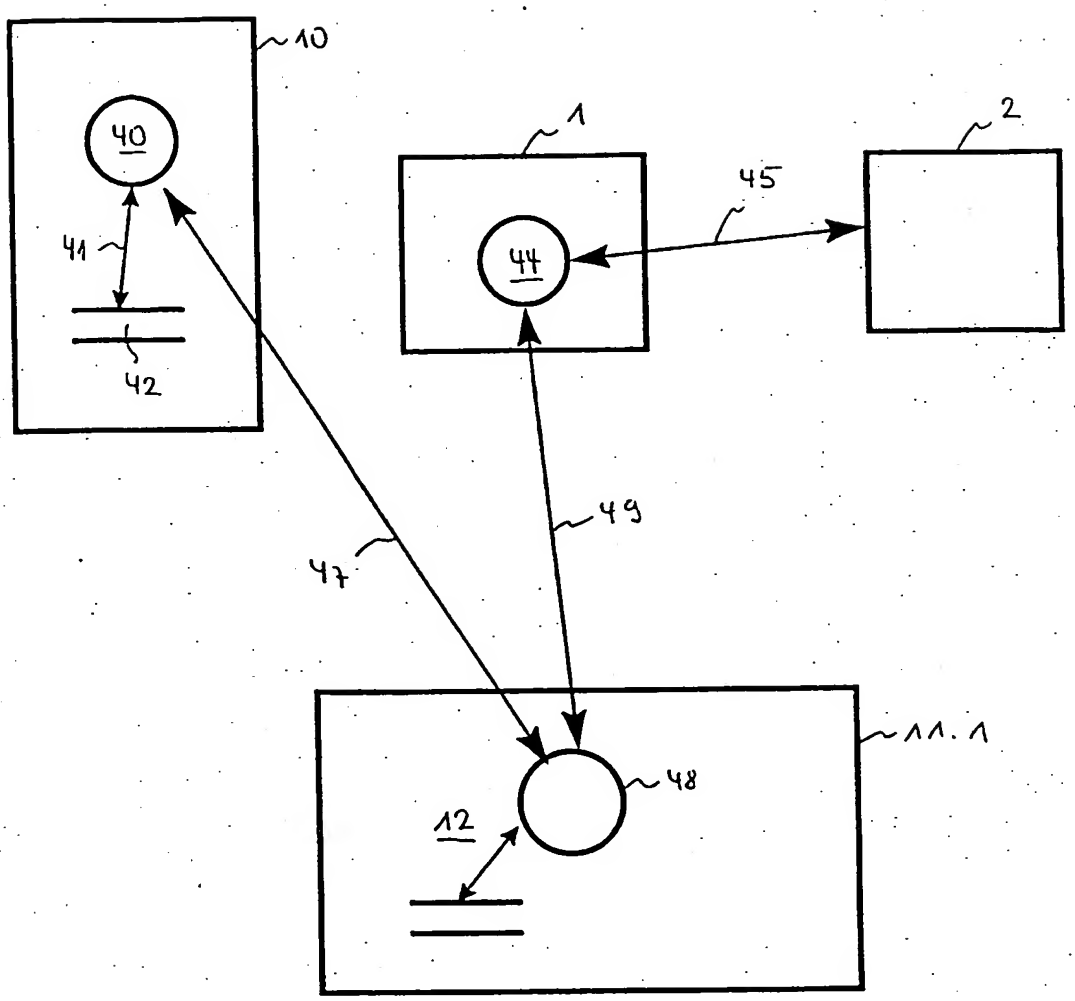


Fig. 6

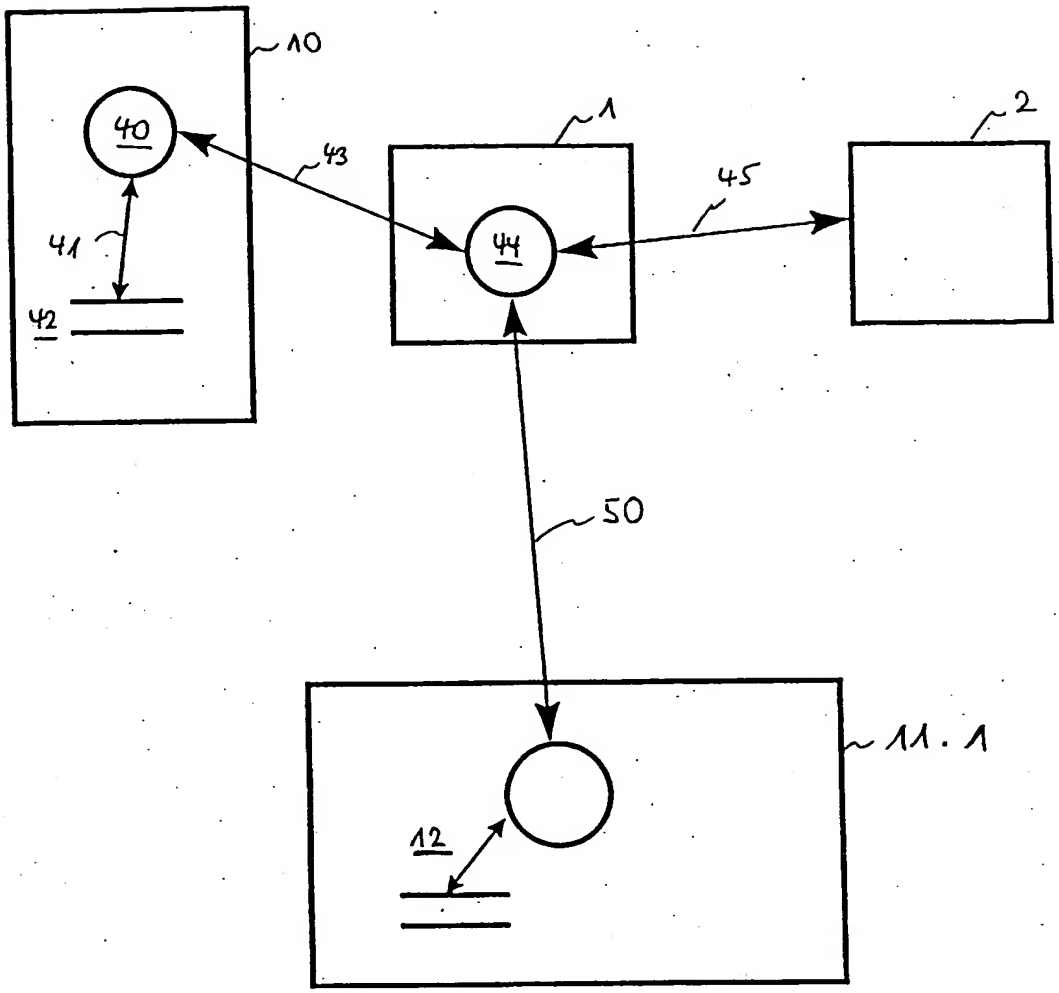


Fig. 7

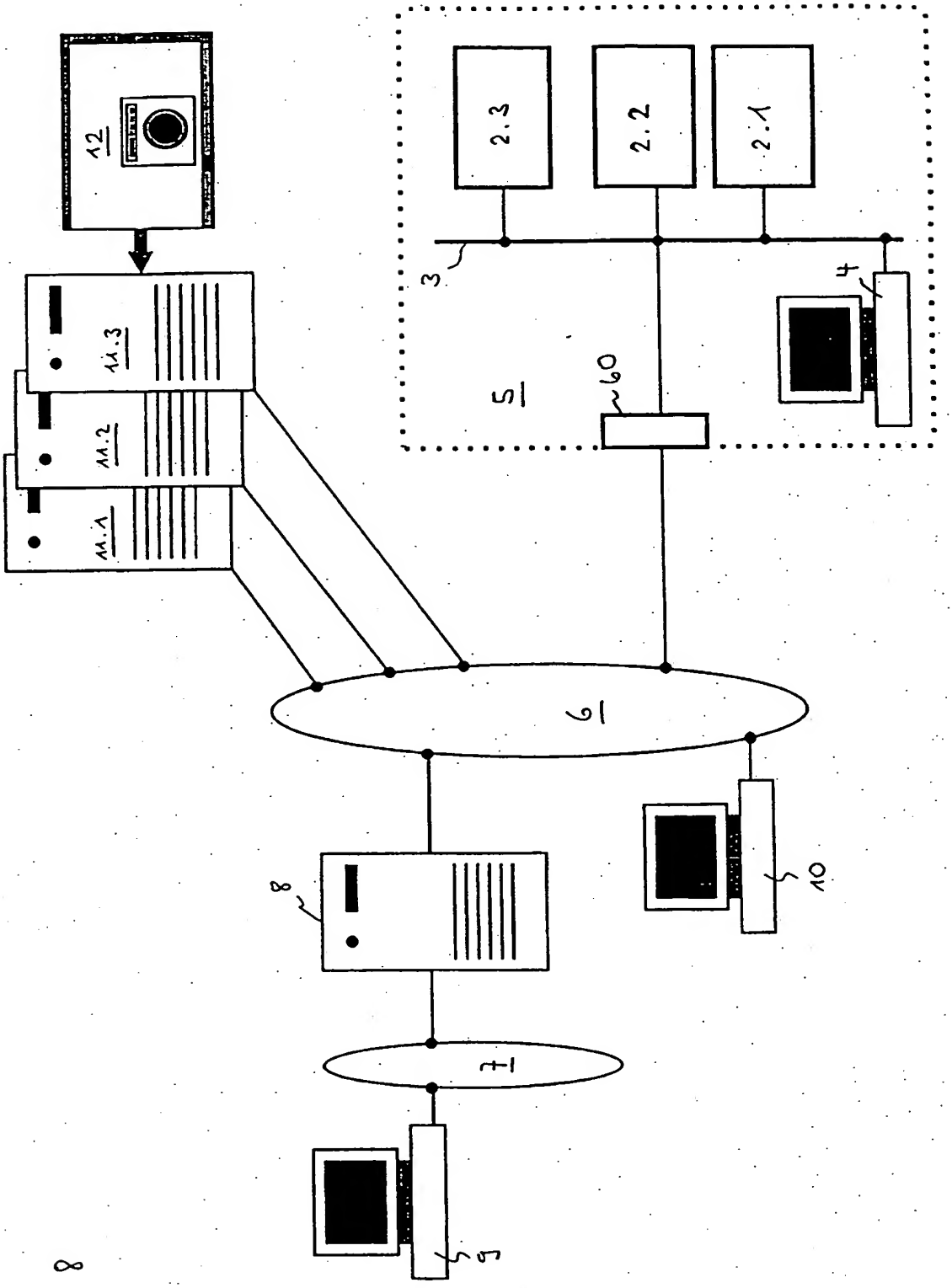


Fig. 8

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 96 11 2872

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
X	WO-A-96 20555 (GEMSTAR DEV CORP) 4.Juli 1996 * Zusammenfassung * * Seite 8, Zeile 13 - Zeile 33 * * Seite 9, Zeile 3 - Seite 11, Zeile 9 * * Seite 12, Zeile 20 - Zeile 27 *	1-9	H04L12/28 H04L12/22 H04L29/06
A	WO-A-90 15394 (AISI RESEARCH CORP ;WACKS KENNETH P (US)) 13.Dezember 1990 * das ganze Dokument *	1-9	
D,A	WO-A-96 05681 (SHIVA CORP) 22.Februar 1996 * das ganze Dokument *	1	

RECHERCHIERTE SACHGEBIETE (Int.Cl.6)

H04L
H04M

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	10.Januar 1997	Mikkelsen, C

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

P2809.TRN

Arrangement for access for an apparatus connected to a local network by way of a public network

The invention relates to an arrangement as set forth in the classifying portion of claim 1.

Such arrangements are suitable for example for the remote programming of apparatuses for controlling or regulating air conditioning parameters of a room by way of a public data network or generally for data exchange between a station connected to a public data network and an apparatus which can be accessed by way of the public data network.

An arrangement of that kind is known (WO 9605681 A1) in which a database connected to a local data network can be accessed by way of a server from a station connected to a public data network, by way of the public data network.

Arrangements and methods are also known (EP 686 905 A1 or EP 693 836 A1) by which the authenticity of a data transfer in a public data network can be guaranteed.

The object of the present invention is to provide an arrangement with which the functionality of an apparatus is programmable from a station by way of a public network - for example by way of the Internet - with the required degree of security and with which data of the apparatus can be reliably transmitted by way of the public network and displayed at the station.

In accordance with the invention that object is attained by the features of claim 1. Advantageous configurations are set forth in the appendant claims.

Embodiments of the invention are described in greater detail hereinafter with reference to the drawing in which:

Figure 1 shows an arrangement with apparatuses, the functionality of which is controllable from different stations by way of a public network,

Figure 2 shows an interface device for a controllable apparatus,

Figure 3 shows a unit of the interface device,

Figure 4 shows a data flow chart relating to the arrangement,

Figure 5 shows the data flow in a first variant of the arrangement,

Figure 6 shows the data flow of a second variant of the arrangement,

Figure 7 shows the data flow of a third variant of the arrangement, and

Figure 8 shows a variant of the interface device.

In Figure 1 reference numeral 1 denotes an interface device for an apparatus 2 which typically is a device 2.1 for controlling or regulating an air conditioning parameter of a room or a building or a video recorder 2.2 or a washing machine 2.3.

In an advantageous design of the arrangement the apparatus 2 or 2.1, 2.2 or 2.3 is connected by the interface device 1 to a communication medium 3 which is advantageously also connected to a terminal 4. The communication medium 3, the terminal 4 and the units 2.1, 2.2 and 2.3 of the apparatus 2 form a local data communication network 5. The communication medium 3 of the local data communication network 5 is typically a house bus. In general the communication medium 3 is a wire connection or a wireless connection.

The terminal 4 is preferably a personal computer.

The local data communication network 5 is connected to a public data communication network 6. Typically at least one further local data communication network 7 is connected by way of a communication computer 8 to the public data communication network 6, at least one further terminal 9 being connected to the data communication network 7.

The interface device 1 is advantageously so designed that the apparatus 2 or 2.1, 2.2 or 2.3 can be accessed both from the terminal 4 of the local data communication network 5 and from the terminal 9 of the further local data communication network 8 or from any station 10 connected to the public data communication network 6 for reliable data exchange.

It is advantageously possible by way of the public data communication network 6 to reach at least one further computer unit 11.1, 11.2 or 11.3 at which is stored a database 12 associated with the apparatus 2, 2.1, 2.2 or 2.3, wherein data of the database 12 can be represented at least in extract-wise fashion in an output window on the terminal 4 or 9 and also the station 10.

The interface device 1 has a security module 20 (Figure 2) which is advantageously connected to a first communication module 21 and a second communication module 22, wherein the first communication module 21 is at least a part of the interface between the security module 20 and the communication medium 3 and the second communication module 22 is at least a part of the interface between the security module 20 and the apparatus 2, 2.1, 2.2 or 2.3.

If the communication medium 3 is an electrical line the interface device 1 also has a suitable plug element 23 for connection of the interface device 1 to the communication medium 3 (Figure 1). The interface device 1 can typically be connected by way of a further plug element 24 to the apparatus 2 or 2.1, 2.2 or 2.3. If necessary however the interface device 1 may not be connected to the apparatus 2 or 2.1,

2.2 or 2.3 galvanically by way of the further plug element 24, but in a different fashion, for example by way of a modulatable light beam.

It will be appreciated that the nature of the communication modules 21 and 22 is matched to the transmission protocols involved and the transmission means employed. The first communication module 21 is for example an electronic unit for implementing the protocol TCP/IP (Transmission Control Protocol/Internet Protocol) while the second communication module 22 is for example an electronic unit for implementing the transmission protocol of the so-called PROFIBUS (Process Field Bus; DIN 19 245).

The security module 20 advantageously includes first means 31 (Figure 3) for operation of the first communication module 21 (Figure 2), second means 32 (Figure 3) for operation of the second communication module 22 (Figure 2), third means 33 (Figure 3) for decoding of a network address, fourth means 34 for encoding and decoding of data and fifth means 35 for interpreting and executing commands which are directed to the apparatus 2 or 2.1, 2.2 or 2.3 which is connected to the interface device 1.

Figure 4, Figure 5, Figure 6 and Figure 7 show the essential data flows between the station 10, the interface device 1 and the apparatus 2, while Figures 5 to 7 also include the database 12 embodied in the computer unit 11.1 or 11.2 or 11.3 (Figure 1).

In the mode of representation for data flow charts which is known from the literature and which has been adopted for Figures 4 to 7 (see in that respect for example D. J. Hatley, I. A. Pirbhai: Strategies for Real-Time System Specification, Dorset House, NY 1988), a circle denotes an activity, a square generally denotes a system and an arrow denotes a channel for the transmission of data and/or events, wherein an arrowhead points in the substantial data flow direction. A data store which is generally available to a plurality of activities is represented by two parallel lines of equal length. The term data store is used here to denote a device for the storage of data, which also has means for preventing conflicts in the event of time-parallel access of a plurality of activities to the data. In addition for example an arrangement comprising two activities connected by a channel is equivalent to a single activity which performs all tasks of said two activities. An activity can generally be broken down into a plurality of activities which are connected by way of channels and/or data stores. Further terms used in the literature relating to data flow charts are "terminator" for the adjoining system, "process" or "task" for the activity, "data flow" or "channel" for the channel and "pool" or "data pool" for the data store.

An activity can be embodied as an electronic circuit or also in software terms as a process, program portion or routine, while in the

case of a software implementation the activity also involves target hardware.

The station 10 has a first activity 40 and advantageously a first data store 42 connected to the first activity 40 by way of a channel 41 for the storage of information for cryptographic methods.

A command B for the apparatus 2 which is inputted by an operator of the station 10 is transmitted, encoded by the first activity 40 with known cryptographic methods, by way of a channel 43 to a second activity 44 embodied in the interface device 1, the channel 43 being formed by way of the public data communication network 6 (Figure 1). The command B transmitted to the second activity 44 is interpreted and executed by the second activity 44 preparing a certain data telegram T which is matched to properties of the apparatus 2, and transmitting it by way of a channel 45 to the apparatus 2. If necessary an answer from the apparatus 2 to the data telegram T is transmitted by way of the channel 45 to the interface device 1 and from there by way of the channel 43 to the station 10.

To provide protection from possible improper use the data exchanged between the station 10 and the interface device 1 are advantageously transmitted in the public data communication network 6 in encoded form in such a way that the authenticity of the data is also safeguarded. A high security standard for remote operation can be achieved by the functionality of the security module 20, such functionality including in particular with the first means 31 (Figure 3) and the second means 32 encoding/decoding of protocols and with the means 34 cryptographic methods for the transmission of data by way of the public data communication network 6.

The database 12 which is available by way of the public data communication network 6 (Figure 1) can be used for operator-friendly user guidance at the station 10.

The database 12 stores essential data relating to operation, programming and control of the apparatus 2 or 2.1 or 2.2 or 2.3. The database is set up for example by the manufacturer of the apparatus 2 or 2.1 or 2.2 or 2.3 in the public data communication network 6 and remote operation is made available to users of the apparatus 2 or 2.1 or 2.2 or 2.3.

In an advantageous configuration of the database 12 the data necessary for operation, programming and control of the apparatus 2 or 2.1 or 2.2 or 2.3 can be inspected in clearly reviewable form from the station 10 and if necessary can be altered by the user of the station 10. If the public data communication network 6 is the Internet at least a part of the database is advantageously available as so-called websites.

In a first variant (Figure 5) of the arrangement a channel 46 is formed from the first activity 40 by way of the public data communication network 6 to the database 12. The database 12 which is available by way of the channel 46 permits operation-friendly user guidance at the station 10. The channels 43 and 45 which can be formed between the station 10 and the apparatus 2 are bidirectional so that it is also possible for current apparatus data to be displayed at the station 10.

In a second variant (Figure 6) of the arrangement a channel 47 is formed from the first activity 40 by way of the public data communication network 6 to the database 12. A command transmitted from the station 10 to the database 12 for operation, programming or control of the apparatus 2 or 2.1 or 2.2 or 2.3 is produced by an activity 48 associated with the database 12 and transmitted by way of a further channel 49 to the interface device 1 and from there to the apparatus 2, the channels 47, 49 and 45 being bidirectional so that current apparatus data can also be displayed at the station 10.

In a third variant (Figure 7) of the arrangement operator-friendly user guidance at the station 10 is made possible by virtue of the fact that the second activity 44 embodied in the interface device 1 forms a channel 50 to the database 12.

Instead of the station 10 shown in Figure 5, Figure 6 and Figure 7, it will be appreciated that the terminal 4 (Figure 1) and the further terminal 9 can also be used for operation, programming and control of the apparatus 2 or 2.1 or 2.2 or 2.3.

The interface device 1 with the security module 20 permits secure, inexpensive and user-friendly remote operation, remote programming and remote control of the apparatus 2 or 2.1 or 2.2 or 2.3 by way of the public data communication network 6. The security module 20 can be produced in the form of a highly integrated component. The security module 20 can be entirely embodied in the form of a so-called hardware chip, whereby the degree of security that can be achieved can be substantially enhanced.

In Figure 8 reference numeral 60 denotes an alternative configuration of the interface device 1 (Figure 1). The alternative configuration 60 basically involves the functionality shown in Figure 3, but it is designed in such a way that it can be functionally inserted between the public data communication network 6 and the local data communication network 5. The alternative configuration 60 of the interface unit is advantageous in particular when the apparatuses 2 or 2.1, 2.2 and 2.3 to be operated, of the local data communication network 5, have similar operational concepts.

The proposed arrangement with the interface device 1 or 60 for access to the apparatus 2 permits secure remote programming in

particular also of apparatuses or parts of an installation, in which respect reference may be made by way of example to heating, ventilation and air conditioning installations, access and fire monitoring systems or in general terms building automation installations which are also referred to as building management systems.

CLAIMS

1. An arrangement for access to an apparatus (2.1; 2.2; 2.3) connected to a local network (5), by way of a station (10; 9; 4) connected to a public network (6), the local network (5) being connected to the public network (6),

characterised by

an interface device (1; 60) by way of which the apparatus (2.1; 2.2; 2.3) can be accessed for data exchange, wherein the interface device (1; 60) has means (35) for interpreting and executing a command which can be produced by way of the station (10; 9; 4) connected to the public network and by which the functionality of the apparatus (2.1; 2.2; 2.3) is controllable or programmable or by which data of the apparatus (2.1; 2.2; 2.3) can be interrogated, and

wherein the interface device (1; 60) also has means (34) for checking the authenticity of the command.

2. An arrangement according to claim 1 characterised in that the interface device (1; 60) and the station (10; 9; 4) have means (40, 42; 34) for encoding and decoding data so that a data flow transmitted between the station (10; 9; 4) and the interface device (1) by way of the public network (6) can be encoded.

3. An arrangement according to one of the preceding claims characterised in that a database (12) which can be accessed by way of the public network (6) and which has data for the guidance of an operator of the station (10; 9; 4) is available.

4. An arrangement according to one of the preceding claims characterised in that a command set which can be interpreted by the interface device (1; 60) is available in a database (12) which can be accessed by way of the public network (6).

5. An arrangement according to one of the preceding claims characterised in that the interface device (1; 60) has means (21, 31) for encoding/decoding a protocol for the transmission of data by way of the public network (6).

6. An arrangement according to one of the preceding claims characterised in that the interface device (1; 60) has means (22, 32) for communication with the apparatus (2.1; 2.2; 2.3).

7. An arrangement according to one of the preceding claims characterised in that the apparatus (2.1) has a means for controlling or regulating air conditioning parameters of a room.

8. An arrangement according to one of the preceding claims characterised in that the interface device (1) is connected between the communication medium (3) and the apparatus (2.1; 2.2; 2.3).

9. An arrangement according to one of the preceding claims characterised in that the interface device (60) is connected between the local communication network (5) and the public data communication network (6).

ABSTRACT

An arrangement for access to an apparatus (2.1; 2.2; 2.3) connected to a local network (5), by way of a station (10; 9; 4) connected to a public network (6) has an interface device (1) by way of which the apparatus (2.1; 2.2; 2.3) can be accessed for data exchange, wherein the interface device (1) has means for interpreting and executing a command which can be produced by way of the station (10; 9; 4) connected to the public network and by which the functionality of the apparatus (2.1; 2.2; 2.3) is controllable or programmable or by which data of the apparatus (2.1; 2.2; 2.3) can be interrogated. The interface device (1) also has means for checking the authenticity of the command. The arrangement permits secure remote programming in particular also of apparatuses or parts of an installation by way of a public network (6), in which respect mention may be made by way of example of heating, ventilating and air-conditioning installations, access and fire monitoring systems or generally building automation installations which are also referred to as building management systems.

(Figure 1)